NTTデータ先端技術株式会社

Oracle Java SE JDK および JRE の Rhino スクリプトエンジンの脆弱性（CVE-2011-3544）に関する検証レポート

2011/12/2
NTT データ先端技術株式会社
辻　伸弘
渡邊　尚道
小田切　秀暁

【概要】

Oracle Java SE の JDK および JRE に、Rhino スクリプトエンジンによる、任意のコードが実行可能な脆弱性(CVE-2011-3544)が存在することが発見されました。この脆弱性は、Java 内に組み込まれた JavaScript エンジンが JavaScript エラーオブジェクトを適切に処理しません。

この脆弱性により、細工された Web ページの閲覧などで、使用した Web ブラウザの実行ユーザ権限と同じ権限が奪取される危険性があります。
想定される被害としては、奪取されたユーザ権限による情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、Oracle Java SE JDK および JRE の脆弱性（CVE-2011-3544）の再現性について検証を行いました。

【影響を受けるとされているアプリケーション】

影響を受ける可能性が報告されているのは次の通りです。

- Oracle Java SE JDK および JRE 7
- Oracle Java SE JDK および JRE 6 Update 27 以前のバージョン

【対策案】

JDK および JRE のアップデートを実施いただく事を推奨いたします。

- Oracle Java SE JDK および JRE 7 Update 1
- Oracle Java SE JDK および JRE 6 Update 29

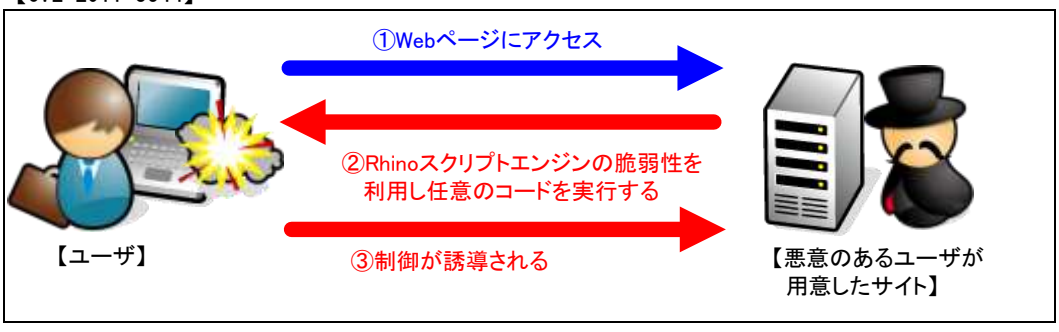
【参考サイト】

Oracle Java SE Critical Patch Update Advisory - October 2011
http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html

CVE-2011-3544
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3544

【検証イメージ】

【CVE-2011-3544】



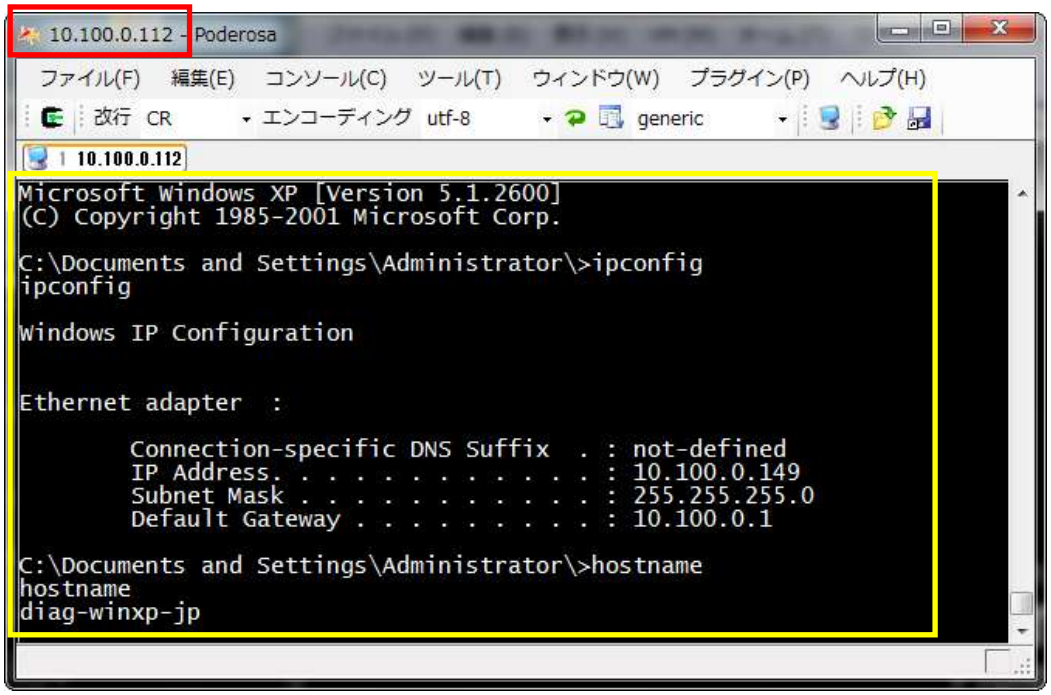
NTTデータ先端技術株式会社

【検証ターゲットシステム】
Windows XP SP3 IE7 JRE 6 Update 23

【検証概要】
ターゲットシステムに、細工した Web コンテンツをロードさせることで任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊ 誘導先のシステムは Debian 5.05 です。

【検証結果】
下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（Debian）のコンソール上にターゲットシステム（Windows XP）のプロンプトが表示されています。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、コマンドを実行した結果が表示されています。これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムの制御の奪取に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部　営業担当　営業企画グループ
TEL:03-5425-1954
http://security.intellilink.co.jp/